Journal of Law, Policy and Globalization
ISSN 2224-3240 (Paper) ISSN 2224-3259 (Online)
Vol.152, 2026

Protection of Critical National Information Infrastructure Against Cyber Attacks: An Evaluation of The Legal and Regulatory Framework in Nigeria

KELVIN BRIBENA PhD
Faculty of Law, Niger Delta University,
Wilberforce Island, Bayelsa State, Nigeria.

Abstract
The rapid digital transformation of contemporary societies has made information systems and communication networks essential components of national security, economic development, public administration and social stability. In Nigeria, critical sectors including banking, telecommunications, energy, healthcare, defence, transportation and government administration increasingly depend on interconnected digital infrastructure. While this digital dependency has enhanced efficiency and innovation, it has simultaneously created significant vulnerabilities to cyber attacks capable of disrupting essential services, compromising sensitive information and undermining national security. Critical National Information Infrastructure (CNII) has therefore emerged as a strategic national asset requiring effective legal protection. This study evaluated Nigeria's legal and regulatory framework for protecting Critical National Information Infrastructure against cyber attacks. It examined the constitutional foundations of cybersecurity protection, by examining the extant laws like the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 as amended in 2024 and other relevant institutions including sector-specific regulators. The study employed the doctrinal research methodology by evaluating primary and secondary sources of relevant laws and declassified policy documents. The study found that although Nigeria has established important legal foundations for cybersecurity governance, the current framework remains too fragmented and inadequate to address the complexity of contemporary cyber threats targeting critical national information infrastructure. The study identified major weaknesses including the absence of a dedicated Critical National Information Infrastructure Protection Act, insufficient cybersecurity obligations for infrastructure operators, weak incident reporting mechanisms, institutional overlap, limited technical capacity and challenges associated with cross-border cybercrime enforcement. The study concluded with recommendations that Nigeria's ability to protect its critical digital infrastructure will depend on moving beyond a reactive cybercrime framework towards a comprehensive and preventive governance model capable of securing digital infrastructure while protecting constitutional rights and supporting technological innovation.

Keywords: Critical National Information Infrastructure, Cybersecurity, Cyber Attacks, Nigeria, Cybercrime Law, National Security, Data Protection, Digital Infrastructure.

DOI: 10.7176/JLPG/152-10

Publication date: May 28th 2026

1. Introduction

The increasing integration of digital technologies into national development has transformed information infrastructure into one of the most valuable assets of modern states. Governments, businesses and individuals now depend heavily on digital systems for communication, financial transactions, healthcare delivery, energy management, transportation services, public administration and national security operations. This transformation has created significant opportunities for economic growth and social development, but it has also generated new security vulnerabilities. Information systems that support essential services have become attractive targets for cybercriminals, terrorist organisations, hostile state actors and other malicious actors seeking financial, political or strategic advantages.[1]

Critical National Information Infrastructure (CNII) represents the digital foundation upon which essential national services operate. Unlike ordinary information systems, CNII possesses strategic significance because its disruption may produce consequences extending beyond individual organisations to affect national security,

[1] Convention on Cybercrime (Budapest Convention), opened for signature 23 November 2001, ETS No 185.

economic stability, public safety and social order. A successful cyber-attack against a national payment system, electricity management network, telecommunications infrastructure or government database may therefore generate consequences comparable to attacks against traditional physical infrastructure.

The protection of CNII has become particularly important in Nigeria due to the country's rapid digital transformation. Nigeria has developed one of Africa's largest digital economies, supported by widespread mobile telecommunications, financial technology innovation, electronic banking, digital identity systems, online government services and cloud-based information platforms. The growth of fintech companies, mobile payment systems and digital public infrastructure has increased efficiency and financial inclusion, but it has also expanded the country's exposure to cyber risks.

Cyber threats affecting Nigeria's digital ecosystem have become increasingly sophisticated. Financial institutions have experienced phishing attacks, malware infections, identity theft and unauthorised access to electronic banking systems. Telecommunications networks face threats involving service disruption, subscriber data compromise and infrastructure manipulation. Government databases containing sensitive citizen information remain attractive targets for cybercriminals seeking identity information or strategic intelligence. Similarly, energy infrastructure increasingly depends on digital control systems that may be vulnerable to cyber exploitation.

The legal protection of CNII therefore raises fundamental questions concerning the adequacy of Nigeria's cybersecurity framework. Traditional criminal law approaches, which focus primarily on punishing offenders after cyber incidents occur, are insufficient for addressing modern cyber threats. Effective CNII protection requires a comprehensive governance framework involving preventive obligations, cybersecurity standards, risk assessment procedures, incident reporting requirements, resilience planning and coordinated responses among government agencies and private sector operators.

Nigeria's principal cybersecurity legislation is the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, which was enacted to provide a comprehensive legal framework for preventing and prosecuting cyber offences. The Act recognises the importance of protecting critical information infrastructure and empowers the President to designate certain computer systems and networks as Critical National Information Infrastructure where their disruption may affect national security, economic activities or public welfare.[1] The 2024 amendment to the Act further strengthened aspects of Nigeria's cybersecurity framework by improving reporting obligations, institutional responsibilities and alignment with data protection principles.

However, the Cybercrimes Act remains primarily a cybercrime prevention statute rather than a comprehensive CNII protection framework. It criminalises harmful conduct but provides limited guidance regarding the proactive cybersecurity responsibilities of infrastructure operators. Modern critical infrastructure protection requires organisations to implement continuous risk management, cybersecurity audits, vulnerability assessments, incident response plans and recovery strategies. These obligations require more detailed regulatory mechanisms than currently exist.

Nigeria's cybersecurity framework is further supported by the Nigeria Data Protection Act 2023, which provides important safeguards regarding information security, confidentiality and protection of personal data. Since many CNII operators process large amounts of personal information, data protection principles contribute significantly to cybersecurity resilience. However, data protection law primarily focuses on privacy and personal information rather than the broader operational security of critical infrastructure.

The institutional framework for cybersecurity governance in Nigeria involves several bodies, including the Office of the National Security Adviser (ONSA), National Information Technology Development Agency (NITDA), Nigeria Data Protection Commission (NDPC), Nigerian Communications Commission (NCC), Central Bank of Nigeria (CBN) and other sector-specific regulators. Although these institutions perform important functions, overlapping responsibilities and limited coordination may affect Nigeria's ability to respond effectively to large-scale cyber incidents.

International developments demonstrate that effective CNII protection requires a comprehensive, risk-based and collaborative approach. The United States has developed a critical infrastructure protection model based on sector coordination, cybersecurity standards and public-private partnerships through institutions such as the Cybersecurity and Infrastructure Security Agency (CISA).[2] Similarly, the European Union's NIS2 Directive

[1] International Telecommunication Union (ITU), *Global Cybersecurity Index 2020* (ITU Publications 2021).
[2] World Economic Forum, *Global Risks Report 2023* (18th edn, World Economic Forum 2023).

establishes binding cybersecurity obligations for operators of essential services, including risk management, incident reporting and regulatory supervision.[1] These models demonstrate that cybersecurity protection requires more than criminal sanctions; it requires continuous governance and resilience-building.

This study evaluates Nigeria's legal and regulatory framework for protecting Critical National Information Infrastructure against cyber-attacks. It argues that while Nigeria has developed important foundations for cybersecurity governance, significant legal and institutional gaps continue to limit effective protection. The study advances three central arguments. First, Nigeria requires a dedicated CNII protection framework capable of establishing clear obligations for infrastructure operators. Secondly, cybersecurity governance must move from a reactive crime-control approach towards a preventive resilience-based model. Thirdly, Nigeria must strengthen institutional coordination, public-private partnerships and international cooperation to effectively address evolving cyber threats.

2. Conceptualising Critical National Information Infrastructure and Cyber Attacks

2.1 Critical National Information Infrastructure

The concept of Critical National Information Infrastructure developed from the recognition that certain information systems are so essential to national functioning that their disruption may cause widespread harm. Traditionally, critical infrastructure referred mainly to physical assets such as electricity networks, transportation systems, water facilities and communication structures. However, technological advancement has created increasing dependence on digital systems, making information infrastructure equally significant. Critical National Information Infrastructure refers to information systems, networks, communication platforms and digital resources whose failure, destruction or compromise would significantly affect national security, economic stability, public health, safety or government operations.[2] The United States Presidential Policy Directive 21 describes critical infrastructure as assets, systems and networks whose destruction or incapacitation would have a debilitating effect on national security, economic stability, public health or safety.[3] This definition has influenced global approaches to infrastructure protection.

In Nigeria, the Cybercrimes Act provides the legal basis for identifying CNII by empowering the President to designate certain computer systems or networks as critical infrastructure where their disruption may affect national interests.[4] Such designation allows government authorities to prescribe additional security measures for their protection. CNII may include:

(a) Financial Infrastructure: Financial systems constitute one of the most important categories of CNII because banking networks, payment platforms and electronic transaction systems support national economic activities. A cyber attack against financial infrastructure may disrupt commerce, compromise customer information and undermine confidence in the financial system.

(b) Telecommunications Infrastructure: Telecommunications networks provide the foundation for digital connectivity. Mobile networks, internet exchange systems and communication platforms support government operations, financial transactions, emergency services and social communication.

(c) Energy Infrastructure: Modern energy systems increasingly rely on digital technologies, including supervisory control and data acquisition systems (SCADA). Cyber attacks against such systems may disrupt electricity generation and distribution, creating economic and security consequences.

(d) Healthcare Infrastructure: Healthcare institutions increasingly rely on electronic medical records, digital health platforms and connected medical devices. Cyber attacks against healthcare systems may compromise sensitive patient information and disrupt essential healthcare delivery.

(e) Government Information Systems: Government databases containing identity information, taxation records, immigration data and public administration information represent valuable targets for cyber attackers. Compromise of these systems may threaten both individual privacy and national security.

2.2 Cyber Attacks Against Critical National Information Infrastructure

Cyber attacks against CNII involve deliberate attempts to compromise the confidentiality, integrity or availability of information systems supporting essential national services. Unlike conventional crimes, cyber attacks possess unique characteristics including anonymity, geographical independence, speed of execution and the ability to create widespread disruption with relatively limited physical presence.

The threat landscape affecting critical infrastructure has evolved significantly. Attackers now employ sophisticated techniques capable of targeting complex technological environments, exploiting software

[1] European Union Agency for Cybersecurity (ENISA), *Threat Landscape for Critical Infrastructures* (ENISA 2022).
[2] National Cybersecurity Policy and Strategy of Nigeria (2021).
[3] Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (as amended), s 3.
[4] Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (as amended), ss 5–8.

vulnerabilities, manipulating information systems and disrupting essential services. These threats may originate from individual criminals, organised cybercrime groups, terrorist organisations, hacktivists or state-sponsored actors. Common cyber-attacks affecting CNII include:

(a) Malware and Ransomware Attacks: Malware refers to malicious software designed to gain unauthorised access, damage systems, steal information or disrupt operations. Ransomware has become one of the most significant threats to critical infrastructure globally. It involves encrypting organisational data and demanding payment before access is restored. For CNII operators, ransomware attacks can have devastating consequences. An attack against a healthcare information system may prevent access to patient records, while an attack against a financial institution may disrupt electronic transactions. Similarly, ransomware targeting government databases may compromise sensitive national information. Nigeria has experienced increasing exposure to ransomware and malware-related threats due to expanded digital adoption. Organisations operating essential services must therefore implement preventive cybersecurity measures, including system monitoring, regular updates, employee training and incident response planning.

(b) Distributed Denial-of-Service (DDoS) Attacks: Distributed Denial-of-Service attacks occur when attackers overwhelm a network or digital service with excessive traffic, preventing legitimate users from accessing the system. Because modern economies depend heavily on online services, DDoS attacks can create significant operational disruption. For telecommunications companies, government agencies and financial institutions, prolonged service interruption may affect public confidence and economic activities. The increasing use of cloud-based services and internet-connected infrastructure has made DDoS protection a critical aspect of cybersecurity governance.

(c) Data Breaches and Unauthorised Access: Data breaches involve unauthorised access, disclosure, modification or theft of information. CNII operators often hold sensitive information, including financial records, identity information, health data and government records. A successful breach may produce consequences beyond privacy violations. Compromised government databases may threaten national security, while stolen financial information may facilitate fraud and identity theft. The Nigeria Data Protection Act 2023 recognises the importance of preventing unauthorised access and requires data controllers and processors to implement appropriate technical and organisational security measures.[1] However, effective protection of CNII requires broader cybersecurity obligations extending beyond personal data protection.

(d) Advanced Persistent Threats (APTs): Advanced Persistent Threats involve prolonged and targeted cyber intrusions designed to maintain unauthorised access to systems for espionage, sabotage or strategic advantage. These attacks are commonly associated with highly skilled actors, including state-sponsored groups. APTs represent a significant threat to national security because attackers may remain undetected for extended periods while gathering intelligence or preparing disruptive operations. Defence systems, government networks and strategic industries are particularly vulnerable to such attacks.

(e) Artificial Intelligence-Enabled Cyber Attacks: The emergence of artificial intelligence has introduced new dimensions to cybersecurity threats. AI tools can enable attackers to automate phishing campaigns, generate malicious code, create convincing deepfakes and conduct sophisticated social engineering attacks. Conversely, AI can strengthen cybersecurity through automated threat detection, anomaly analysis and incident response. The legal challenge is therefore ensuring that AI systems are developed and deployed securely while preventing malicious exploitation.

For Nigeria, where digital infrastructure is rapidly expanding, AI-related cyber threats require incorporation into future CNII protection frameworks.

3. Constitutional and Human Rights Foundations for CNII Protection in Nigeria

Although the Nigerian Constitution does not expressly mention cybersecurity or Critical National Information Infrastructure, several constitutional provisions provide foundations for protecting digital infrastructure and regulating cyber activities.

3.1 Constitutional Obligation to Protect National Security

Section 14(2)(b) of the Constitution of the Federal Republic of Nigeria 1999 provides that "the security and welfare of the people shall be the primary purpose of government."[2] This constitutional responsibility provides

[1] Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (as amended), ss 38–41.
[2] Chukwuma Okoli and Abiola Sanni, 'Cybercrime Regulation in Nigeria: Challenges and Prospects' (2021) 9 *Journal of African Law and Policy* 45.

justification for governmental measures aimed at protecting essential infrastructure, including digital systems necessary for national security and public welfare. Since modern governance increasingly depends on information systems, protection of CNII forms part of the state's obligation to safeguard citizens and maintain national stability. A cyber-attack capable of disabling financial systems, disrupting electricity supply or compromising government databases may directly affect public welfare. Consequently, cybersecurity regulation may be understood as an extension of the constitutional responsibility of government to protect national interests.

3.2 Right to Privacy and Protection of Digital Information

Section 37 of the Constitution guarantees the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications.[1] Although enacted before widespread internet use and artificial intelligence, the provision remains relevant to contemporary digital environments. CNII operators frequently process large volumes of personal and sensitive information. Banks maintain financial records, telecommunications companies hold subscriber information, healthcare institutions manage medical data, and government agencies maintain identity databases. Cyber-attacks against these systems may violate constitutional privacy rights by exposing citizens' confidential information. Therefore, cybersecurity protection is closely connected to privacy protection. The Nigeria Data Protection Act 2023 expands this constitutional foundation by establishing detailed obligations regarding lawful processing, security safeguards, accountability and individual rights.[2]

3.3 Freedom of Expression and Digital Rights

Cybersecurity measures must also consider constitutional protections relating to freedom of expression and access to information. Section 39 of the Constitution guarantees freedom of expression and the right to receive and impart ideas and information.[3] While government has legitimate interests in preventing cybercrime and protecting critical infrastructure, cybersecurity enforcement should not become a mechanism for unjustified restriction of lawful digital expression. This creates an important legal balance. Excessive regulation may undermine digital rights, while insufficient regulation may allow malicious actors to exploit digital platforms. Effective CNII protection therefore requires cybersecurity measures that comply with constitutional principles of legality, necessity and proportionality.

3.4 Right to Equality and Risks of Digital Exclusion

The Constitution also prohibits discrimination under section 42.[4] This principle has relevance to cybersecurity because unequal access to secure digital infrastructure may reinforce social and economic inequalities. For example, if cybersecurity measures result in exclusion of certain groups from digital financial services, government platforms or online healthcare systems, such measures may create discriminatory outcomes. Similarly, cybersecurity technologies such as biometric authentication systems and automated monitoring tools must be designed carefully to avoid disproportionate impacts on vulnerable populations.

4. The Cybercrimes Act 2015 (as Amended) and the Protection of Critical Information Infrastructure

The Cybercrimes (Prohibition, Prevention, etc.) Act 2015 represents Nigeria's primary legislative framework for addressing cybercrime and cybersecurity threats. Before its enactment, cyber-related offences were addressed through fragmented provisions contained in criminal legislation and sector-specific regulations.

The Act introduced a comprehensive framework for:

- preventing cyber offences;
- prosecuting cybercriminal activities;
- protecting computer systems and networks;
- safeguarding electronic communications;
- promoting cybersecurity awareness;

[1] Oluwatosin Oladapo, 'Cybersecurity and Legal Responses to Cybercrime in Nigeria' (2020) 14 International Journal of Law and Information Technology 120.
[2] Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (as amended), s 3.
[3] Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience* (United States Government, 2013).
[4] National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity* Version 1.1 (NIST 2018).

- protecting critical national information infrastructure.[1]

The significance of the Act lies in its recognition that cyber threats may affect national security and economic stability.

4.1 Designation of Critical National Information Infrastructure

Section 3 of the Cybercrimes Act empowers the President to designate certain computer systems, networks or information infrastructure as Critical National Information Infrastructure where their disruption would affect national security, economic activities or public welfare.[2] Following designation, additional protective measures may be prescribed for such infrastructure. This provision represents an important legal development because it recognises that certain digital systems require enhanced protection due to their national significance. However, the provision is limited because it does not establish a detailed regulatory framework for CNII operators. The Act does not comprehensively prescribe:

- cybersecurity risk assessment obligations;
- mandatory security standards;
- vulnerability management requirements;
- cybersecurity certification;
- mandatory audits;
- recovery and resilience obligations.

Therefore, while section 3 provides the legal foundation for CNII recognition, it does not create a complete protection regime.

4.2 Cybercrime Offences Relevant to CNII Protection

The Cybercrimes Act criminalises several forms of conduct that may threaten CNII.

Unauthorised Access: Section 6 criminalises unlawful access to computer systems and networks.[3] This offence is particularly relevant because many cyber attacks begin with unauthorised entry into digital systems.

System Interference: Section 8 prohibits intentional interference with computer systems, including damaging, deleting, altering or disrupting computer operations.[4] Such conduct directly threatens CNII because disruption of essential systems may affect public services and national security.

Unlawful Interception: Section 7 criminalises unlawful interception of non-public transmissions of computer data.[5] This provision protects communication systems from unauthorised monitoring.

Cyber Terrorism: Section 18 addresses cyber terrorism by criminalising intentional attacks against computer systems where the purpose is to intimidate populations, destabilise government operations or threaten national security.[6] This provision is particularly relevant to CNII because terrorist organisations may increasingly exploit digital systems to create disruption.

4.3 Limitations of the Cybercrimes Act

Despite its importance, the Cybercrimes Act has several limitations. First, it focuses primarily on criminalisation rather than prevention. Modern cybersecurity requires organisations to actively manage risks before attacks occur.

Secondly, the Act does not impose detailed cybersecurity duties on private entities operating critical infrastructure.

Thirdly, enforcement challenges remain significant due to limited technical expertise, resource constraints and difficulties associated with investigating transnational cybercrime.

Fourthly, the Act does not specifically address emerging threats such as artificial intelligence-enabled attacks, cloud infrastructure vulnerabilities and supply-chain cyber risks.

---

[1] Melissa Hathaway, 'Cyber Security: An Economic and National Security Crisis' (2012) *Project Report, Hathaway Global Strategies*.
[2] Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (as amended), s 41.
[3] Office of the National Security Adviser, National Cybersecurity Policy and Strategy 2021.
[4] National Information Technology Development Agency Act 2007.
[5] National Information Technology Development Agency, Nigeria Data Protection Regulation 2019 Implementation Framework.
[6] Nigeria Data Protection Act 2023.

Therefore, while the Cybercrimes Act provides an essential foundation, additional legislation and regulatory measures are required to achieve comprehensive CNII protection.

5. The Nigeria Data Protection Act 2023 and Cybersecurity Obligations for Critical Infrastructure Protection

The enactment of the Nigeria Data Protection Act (NDPA) 2023 represents a significant milestone in Nigeria's digital regulatory development. Although the primary objective of the Act is to establish a comprehensive framework for the protection of personal data and privacy rights, its provisions have important implications for cybersecurity and the protection of Critical National Information Infrastructure (CNII). This relationship exists because most operators of critical infrastructure process substantial volumes of personal, financial, biometric and operational information in the course of providing essential services. Consequently, effective data protection has become an important component of broader cybersecurity resilience.

Contemporary cyber-attacks against critical infrastructure frequently involve attempts to access, manipulate, destroy or disclose sensitive information. A successful cyber-attack against a banking system may expose customers' financial records and authentication details; an attack against telecommunications infrastructure may compromise subscriber information and communication data; while a breach of government databases may expose identity information capable of creating national security concerns. These realities demonstrate that data protection and cybersecurity are increasingly interconnected areas of legal regulation.

The NDPA provides a framework requiring organisations involved in personal data processing to adopt appropriate safeguards, maintain accountability and protect information against unauthorised access, alteration, destruction or disclosure. These obligations contribute to the overall protection of CNII by strengthening information security practices among organisations responsible for operating essential digital systems.

5.1 Scope and Application of the Nigeria Data Protection Act 2023

The Nigeria Data Protection Act 2023 adopts a broad territorial scope designed to regulate personal data processing activities connected with Nigeria. The Act applies where a data controller or processor is domiciled, resident or operating within Nigeria, where processing activities occur within Nigeria, or where processing relates to Nigerian data subjects even where the organisation responsible for processing operates outside Nigerian territory.[1]

This broad application is particularly significant in the context of Critical National Information Infrastructure because many essential digital services depend on multinational technology companies, cloud service providers and foreign technology platforms. For instance, telecommunications operators may rely on international cloud infrastructure for data storage and service delivery, financial institutions may utilise foreign technology vendors for payment processing and cybersecurity solutions, while government institutions may adopt externally developed digital platforms for public administration.

By extending obligations to entities processing Nigerian citizens' personal data regardless of their physical location, the NDPA ensures that foreign organisations involved in Nigeria's digital ecosystem remain subject to Nigerian data protection requirements. This approach is particularly important in an increasingly interconnected digital environment where critical infrastructure operations frequently involve cross-border technology relationships. However, while the NDPA provides significant protection for personal information, it should not be regarded as a complete cybersecurity framework for CNII protection. Critical infrastructure security extends beyond personal data protection and includes operational technology security, industrial control systems, network resilience, software security, supply-chain protection and continuity of essential services. Therefore, the NDPA should be understood as one component of a broader cybersecurity governance structure rather than a standalone mechanism for protecting critical infrastructure.

5.2 Data Security Obligations and CNII Protection

One of the most important contributions of the NDPA to cybersecurity governance is the obligation imposed on data controllers and processors to implement appropriate technical and organisational measures to protect personal information. Section 39 of the Act requires organisations handling personal data to safeguard such information against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, unauthorised access, misuse or other forms of compromise.[2]

[1] Nigeria Data Protection Act 2023, ss 4–5.
[2] Nigerian Communications Act 2003.

The requirement to implement security measures according to the risks associated with processing activities reflects a risk-based approach to data protection. Organisations are expected to adopt appropriate safeguards, including encryption, pseudonymisation, access control mechanisms, system resilience measures, regular security testing, vulnerability assessments and incident response procedures. These obligations directly support CNII protection because many critical infrastructure systems depend on secure management of sensitive information. For example, financial institutions operating electronic payment systems must ensure that customer information, transaction records and authentication mechanisms are protected from cyber compromise. Similarly, healthcare institutions maintaining electronic medical records must establish effective security controls to prevent unauthorised access and ensure confidentiality of patient information. Nevertheless, the NDPA does not establish detailed cybersecurity requirements specifically designed for critical infrastructure operators. The Act does not expressly require CNII operators to adopt comprehensive cyber resilience frameworks, operational technology security standards, mandatory penetration testing regimes, supply-chain risk management procedures or critical infrastructure security audits. Consequently, although the NDPA strengthens information security practices, it cannot independently provide a complete legal framework for CNII protection. Additional legislation and sector-specific regulations remain necessary to address the wider cybersecurity challenges associated with essential digital infrastructure.

5.3 Data Protection Impact Assessments and Critical Infrastructure

The NDPA introduces the concept of Data Protection Impact Assessments (DPIAs) as a mechanism for identifying and managing risks associated with high-risk data processing activities.[1] This requirement is particularly relevant to CNII operators because many critical infrastructure systems involve large-scale processing of sensitive information. Critical infrastructure operators frequently manage information systems involving national identity records, biometric databases, financial transaction information, healthcare records and telecommunications subscriber data. Given the sensitivity and scale of these operations, DPIAs provide an important mechanism for evaluating potential risks and implementing appropriate safeguards before significant harm occurs.

A DPIA requires organisations to examine the nature, scope, context and purposes of processing activities, identify potential risks to individuals' rights and freedoms, and establish measures capable of reducing those risks. This preventive approach represents a significant improvement over traditional regulatory models that respond only after security failures occur. However, the application of DPIAs within CNII protection remains limited because the assessment primarily focuses on privacy risks rather than broader infrastructure security concerns. Critical infrastructure protection requires consideration of additional factors, including operational disruption, national security implications, cyber attack scenarios, system resilience and recovery capabilities. For this reason, Nigeria should consider expanding the DPIA model into broader Cybersecurity and Infrastructure Impact Assessments specifically applicable to CNII operators. Such assessments would enable organisations to evaluate not only privacy risks but also wider consequences associated with cyber attacks against essential infrastructure.

5.4 Automated Decision-Making and Critical Systems

The increasing adoption of artificial intelligence and algorithmic technologies has created new challenges for cybersecurity governance. The NDPA addresses automated decision-making by providing safeguards against situations where individuals are subjected solely to automated decisions, including profiling, where such decisions produce legal or similarly significant consequences unless appropriate protections are established.[2] This provision is increasingly relevant because critical sectors are adopting automated systems to improve efficiency and decision-making. Financial institutions use automated fraud detection systems, banks employ algorithmic credit assessment tools, telecommunications providers utilise automated identity verification technologies, and healthcare organisations increasingly rely on artificial intelligence-assisted decision-making systems. Where automated systems influence access to essential services, individuals should have meaningful safeguards, including the opportunity for human review, the ability to challenge decisions and access to relevant information regarding the operation of such systems. However, the NDPA does not establish a comprehensive algorithmic accountability framework capable of addressing all emerging risks associated with artificial intelligence within CNII environments. The Act does not provide detailed requirements relating to algorithmic transparency, artificial intelligence model auditing, bias assessment or certification of automated systems.

6. National Cybersecurity Policy and Strategy

[1] Nigerian Communications Commission, *Telecommunications Industry Cybersecurity Guidelines*.
[2] Central Bank of Nigeria, *Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers* (2022).

Nigeria's National Cybersecurity Policy and Strategy provides a broader strategic framework for addressing cyber threats and strengthening national cybersecurity resilience. The Strategy recognises cybersecurity as an essential component of national development and identifies protection of critical information infrastructure as a major priority. Unlike traditional approaches that treat cyber threats solely as criminal matters, the Strategy adopts a broader understanding of cybersecurity as a national security, economic and governance issue. It promotes a multi-stakeholder approach involving government institutions, private sector organisations, academic institutions and international partners. The Strategy focuses on strengthening cybersecurity governance, protecting critical information infrastructure, developing cybersecurity capacity, promoting cybersecurity awareness, improving incident response mechanisms and encouraging international cooperation. The inclusion of CNII protection within Nigeria's national cybersecurity strategy demonstrates recognition that attacks against digital infrastructure may have consequences comparable to attacks against physical infrastructure. Cybersecurity is therefore viewed not merely as a technological issue but as an essential element of national resilience.

6.1 Strengths of the National Cybersecurity Strategy

The National Cybersecurity Policy and Strategy provides several important advantages. First, it adopts a comprehensive understanding of cybersecurity by recognising technological, legal, economic and social dimensions. This holistic approach reflects the reality that cybersecurity challenges cannot be addressed solely through technical solutions.

Secondly, the Strategy encourages cooperation between government institutions and private sector operators. This approach is essential because many critical infrastructures are privately owned or operated, meaning that effective protection requires collaboration between public authorities and private organisations.

Thirdly, the Strategy promotes cybersecurity capacity development. This is particularly important because Nigeria continues to face shortages of cybersecurity professionals capable of implementing advanced security measures.

Fourthly, the Strategy recognises the importance of international cooperation. Since cyber threats frequently originate from outside national borders, effective cybersecurity requires collaboration with foreign governments, international organisations and global technology companies.

6.2 Limitations of the National Cybersecurity Strategy

Despite its importance, the National Cybersecurity Policy and Strategy has limitations because policy documents generally lack the same enforceable legal authority as legislation. While the Strategy provides direction and establishes national objectives, it does not automatically create binding obligations for organisations operating critical infrastructure. For example, the Strategy does not independently require CNII operators to adopt specific cybersecurity standards, report cyber incidents within defined timelines, undergo mandatory cybersecurity audits or maintain detailed cyber resilience plans. Consequently, implementation depends largely on institutional commitment, available resources and voluntary compliance. While strategic guidance is valuable, stronger legal mechanisms are required to transform cybersecurity objectives into enforceable responsibilities. A comprehensive CNII protection framework should therefore combine strategic policy direction with binding legislative obligations.

7. Cybersecurity Threats Affecting Critical National Information Infrastructure in Nigeria

The protection of Critical National Information Infrastructure (CNII) in Nigeria is increasingly challenged by the growing sophistication, frequency and complexity of cyber-attacks. The rapid expansion of digital technologies across government institutions, financial services, telecommunications, healthcare and industrial sectors has significantly increased Nigeria's dependence on interconnected information systems. While digital transformation has enhanced efficiency, accessibility and economic development, it has also expanded the potential attack surface available to malicious actors. Cyber-attacks targeting critical infrastructure possess unique characteristics because they can be executed remotely, anonymously and across national borders, thereby creating consequences that extend beyond individual victims to affect national security, economic stability and public confidence.

Unlike conventional attacks against physical infrastructure, cyber-attacks against CNII may occur without immediate physical destruction while still producing significant operational consequences. The disruption of an electronic payment platform, telecommunications network, electricity management system or government database may interfere with essential services and undermine public trust in digital systems. Consequently, effective CNII protection requires a cybersecurity framework that goes beyond criminalising unlawful access or

punishing cyber offenders after attacks occur. It requires a comprehensive resilience-based approach focused on prevention, risk management, threat intelligence sharing, incident response and recovery mechanisms. Nigeria's increasing reliance on digital infrastructure has therefore created an urgent need for a legal and institutional framework capable of addressing emerging cyber threats. Such a framework must recognise that critical infrastructure protection is not merely a technological concern but also a matter of national security, economic governance and public welfare.

7.1 Cyber Threats Against the Nigerian Financial Sector

The financial sector represents one of the most important components of Nigeria's Critical National Information Infrastructure because modern economic activities depend heavily on electronic banking systems, digital payment platforms, automated teller machines, mobile banking applications and financial technology services. The rapid growth of Nigeria's fintech ecosystem has significantly improved financial inclusion and expanded access to banking services, particularly through mobile payment solutions and online financial platforms. However, this increased digital dependence has simultaneously exposed financial institutions to a wide range of cybersecurity risks.[1]

Financial institutions are attractive targets for cyber criminals because they process valuable financial information and manage systems connected to large volumes of monetary transactions. Cyber threats affecting the financial sector include phishing attacks, credential theft, malware infections, ransomware attacks, identity fraud, unauthorised electronic transactions and database breaches. These attacks may compromise customer information, facilitate financial losses and undermine confidence in Nigeria's financial system.[2]

The consequences of cyber-attacks against financial infrastructure extend beyond individual customers or institutions. A major disruption of banking systems could affect commercial activities, interrupt payment services and create broader economic instability. For example, prolonged unavailability of electronic payment platforms may affect businesses, government transactions and everyday economic activities.

Recognising these risks, the Central Bank of Nigeria has introduced cybersecurity guidelines requiring financial institutions to establish cybersecurity governance structures, conduct risk assessments and maintain incident response mechanisms.[3] These regulatory measures demonstrate the importance of sector-specific cybersecurity obligations in protecting critical infrastructure. However, the relatively advanced cybersecurity framework within the financial sector creates regulatory imbalance because other CNII sectors do not possess equivalent mandatory cybersecurity requirements. Since critical infrastructure systems are interconnected, weaknesses within one sector may create vulnerabilities capable of affecting other sectors. Therefore, Nigeria requires a harmonised cybersecurity framework that establishes minimum protection standards across all categories of CNII.[4]

7.2 Telecommunications Infrastructure and Cybersecurity Risks

Telecommunications infrastructure constitutes one of the most essential categories of CNII in Nigeria because it provides the foundation upon which many digital services operate. Mobile networks, internet service providers and communication platforms support banking services, government administration, healthcare delivery, education, emergency response systems and commercial activities. The widespread adoption of mobile communication technologies has transformed Nigeria into one of Africa's largest telecommunications markets, but it has also created significant cybersecurity vulnerabilities.[5]

The strategic importance of telecommunications infrastructure makes it a valuable target for cyber attackers. Any disruption to communication networks may produce widespread consequences affecting individuals, businesses and government operations. Cyber attackers may attempt to compromise telecommunications infrastructure through network disruption, malware infections, exploitation of software vulnerabilities or unauthorised access to network management systems.

One significant threat is distributed denial-of-service (DDoS) attacks, where malicious actors overwhelm communication networks with excessive traffic, preventing legitimate users from accessing services. A

[1] Central Bank of Nigeria, *Financial Stability Report* (2022).
[2] Financial Action Task Force (FATF), *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (2021).
[3] Nigeria Data Protection Act 2023, s 39.
[4] Bank for International Settlements, *Cyber-resilience: Range of Practices* (BIS 2018).
[5] International Telecommunication Union, *Global Cybersecurity Index 2020*.

prolonged telecommunications outage could disrupt emergency communication, financial transactions, government activities and commercial operations.

Another major concern is the compromise of subscriber information. Telecommunications operators maintain extensive databases containing personal information, identification details, communication records and subscriber activity data. Unauthorised access to such information may result in identity theft, financial fraud, privacy violations and national security risks.

Cyber attackers may also attempt to manipulate telecommunications infrastructure by compromising network management systems. Such attacks could allow criminals to interfere with communication services, intercept information or gain access to sensitive systems. Given the central role telecommunications plays in Nigeria's digital ecosystem, cybersecurity protection within this sector requires continuous monitoring, regulatory supervision, threat intelligence sharing and investment in resilient network architecture.

7.3 Energy Sector Vulnerabilities

The energy sector represents another critical component of Nigeria's national infrastructure because electricity generation, transmission and distribution increasingly depend on digital technologies. Modern energy systems utilise automated monitoring and control technologies, including Supervisory Control and Data Acquisition (SCADA) systems, to improve efficiency and operational management. Although these technologies provide significant benefits, they also introduce cybersecurity vulnerabilities that may be exploited by malicious actors.[1]

Cyber attacks against energy infrastructure may produce consequences that extend beyond information security concerns. Unlike ordinary data breaches, attacks against energy systems may affect physical operations and disrupt essential services. Potential consequences include electricity outages, equipment damage, economic losses and threats to public safety.

Globally, cyber attacks against energy infrastructure have demonstrated the destructive potential of targeting digitally controlled industrial systems. The increasing adoption of smart grids, interconnected devices and automated energy management systems means that cybersecurity must become an essential component of energy regulation and infrastructure planning.

In Nigeria, protection of energy infrastructure requires cooperation between cybersecurity authorities and energy regulators. Traditional physical security measures alone are insufficient because modern energy systems can be compromised through remote digital attacks. Effective protection requires implementation of cybersecurity standards, continuous vulnerability assessment, employee training and incident response planning.

7.4 Healthcare Information Infrastructure

Healthcare information infrastructure has become increasingly dependent on digital technologies, including electronic health records, hospital management systems and connected medical devices. These technologies have improved healthcare administration, patient management and service delivery. However, increased digitalisation has also created new cybersecurity vulnerabilities. Healthcare information represents an attractive target for cyber attackers because it contains valuable personal and medical information. Patient records may be exploited for financial fraud, identity theft or other malicious purposes. Cyber attackers may also target healthcare institutions to disrupt operations, demand ransom payments or obtain sensitive information.

Cyber attacks against healthcare CNII may result in exposure of patient records, interruption of medical services, manipulation of health information and operational disruption. Such consequences may directly affect patient safety and public confidence in healthcare systems. The experience of the COVID-19 pandemic demonstrated the importance of resilient digital healthcare infrastructure. As Nigeria continues to expand digital health initiatives, cybersecurity protection must become integrated into healthcare governance frameworks. Healthcare institutions should therefore adopt comprehensive security measures, including encryption mechanisms, access controls, cybersecurity awareness training, incident response procedures and regular security assessments. Protecting healthcare information infrastructure requires balancing technological innovation with effective security governance.

7.5 Government Digital Infrastructure

Government digital infrastructure represents an essential component of CNII because it supports public administration, national identity management, taxation, immigration systems, electoral processes and national security operations. As government institutions increasingly adopt digital platforms to improve efficiency and service delivery, the protection of these systems has become a significant cybersecurity priority. Government

[1] Nigerian Communications Commission, *Industry Statistics and Cybersecurity Reports*.

databases often contain sensitive information relating to citizens, including identity records, financial information, immigration details and security-related data. Cyber attacks against these systems may therefore produce serious consequences, including compromise of personal information, disruption of public services, threats to national security and loss of public confidence. Examples of government digital infrastructure requiring protection include national identity databases, electoral information systems, immigration platforms, tax administration systems and government communication networks. Although digitalisation has improved accessibility and efficiency in public administration, it has also increased cybersecurity responsibilities. Government agencies must therefore adopt stronger cybersecurity governance practices based on security-by-design principles, regular vulnerability assessments, access management controls, encryption mechanisms and cybersecurity awareness programmes.

8. Legal and Regulatory Gaps in Nigeria's Critical National Information Infrastructure Protection Framework

Although Nigeria has made considerable progress in developing a cybersecurity governance framework through the enactment of the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (as amended), the Nigeria Data Protection Act 2023, national cybersecurity policies and sector-specific regulatory measures, significant legal and institutional weaknesses continue to limit the effectiveness of Critical National Information Infrastructure (CNII) protection. The current framework provides important foundations for addressing cyber threats, but it remains fragmented and insufficiently focused on the unique security requirements of critical infrastructure systems. The nature of contemporary cyber threats requires a regulatory approach that goes beyond criminalising unauthorised access, data breaches or malicious cyber activities.[1] Effective CNII protection requires preventive obligations, continuous risk management, mandatory security standards, coordinated institutional responsibility and mechanisms for ensuring operational resilience. However, Nigeria's existing legal framework does not yet fully establish these requirements. The absence of a comprehensive CNII-specific regulatory regime creates uncertainty regarding the responsibilities of infrastructure operators, the role of government institutions and the minimum cybersecurity standards required for protecting essential digital systems. Consequently, Nigeria's cybersecurity architecture requires further legal reform to address these gaps and develop a more resilient national infrastructure protection framework.

8.1 Absence of Dedicated Critical National Information Infrastructure Legislation

The most significant weakness in Nigeria's cybersecurity framework is the absence of a dedicated Critical National Information Infrastructure Protection Act. Although section 3 of the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 recognises the importance of critical infrastructure by empowering the President to designate certain computer systems and networks as critical national information infrastructure, the provision does not establish a comprehensive regulatory framework for protecting such infrastructure.

The Cybercrimes Act primarily focuses on defining cyber offences, establishing criminal liabilities and providing mechanisms for investigation and prosecution. While these functions are important, they do not adequately address the broader preventive and resilience requirements necessary for protecting critical infrastructure. Cyber attacks against CNII cannot be effectively managed through criminal law alone because many vulnerabilities arise from inadequate security practices, weak governance structures and insufficient risk management.[2]

A dedicated CNII Protection Act would provide greater legal certainty by establishing a specialised framework for identifying, regulating and protecting critical infrastructure systems. Such legislation should provide clear procedures for the identification and classification of critical infrastructure based on factors such as national security significance, economic importance, dependence of essential services, population impact and the consequences of potential disruption.

Furthermore, a comprehensive CNII law should clearly define the responsibilities of infrastructure operators, including obligations relating to cybersecurity risk management, minimum security standards, mandatory security audits, incident reporting requirements, resilience planning and regulatory oversight mechanisms.

The absence of dedicated legislation means that CNII protection currently depends largely on general cybersecurity laws and sector-specific regulations. While such measures provide some level of protection, they create inconsistency because different sectors may operate under varying cybersecurity expectations. A

[1] Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (as amended), s 3.
[2] OECD, *Recommendation on Digital Security of Critical Activities* (OECD 2019).

specialised CNII protection framework would therefore provide a unified national approach while allowing sector-specific adaptation.

8.2 Limited Mandatory Cybersecurity Obligations

Another significant weakness in Nigeria's CNII protection framework is the limited extent of mandatory cybersecurity obligations imposed on critical infrastructure operators. Modern cybersecurity regulation increasingly recognises that organisations responsible for essential services must adopt proactive security measures rather than merely respond to cyber-attacks after they occur.[1] However, Nigerian law does not generally impose comprehensive obligations requiring CNII operators to conduct regular penetration testing, undertake cybersecurity maturity assessments, maintain cyber recovery plans or comply with internationally recognised cybersecurity standards.

The absence of such obligations creates a regulatory environment where cybersecurity practices may vary significantly among infrastructure operators. Some organisations may adopt advanced security measures voluntarily, while others may maintain inadequate protection due to financial limitations, lack of expertise or insufficient regulatory pressure. A reactive cybersecurity approach, which focuses mainly on criminalising cyber-attacks and punishing offenders, is insufficient because many cyber incidents can be prevented through effective risk identification, vulnerability management and organisational preparedness. Critical infrastructure protection requires operators to assume proactive responsibility for securing their systems.

Nigeria should therefore adopt a regulatory approach similar to the European Union's NIS2 Directive, which imposes positive cybersecurity obligations on operators of essential services. Such an approach would require CNII operators to implement appropriate risk management measures, maintain security governance structures and demonstrate continuous compliance with cybersecurity requirements.[2] The introduction of mandatory cybersecurity obligations would transform cybersecurity from a voluntary organisational practice into a legally recognised responsibility for entities whose operations affect national security and public welfare.

8.3 Weak Cyber Incident Reporting Framework

Timely reporting of cyber incidents is a fundamental component of effective national cybersecurity response. Early notification enables authorities to understand emerging threats, coordinate responses and prevent similar attacks against other organisations. However, Nigeria currently lacks a comprehensive mandatory cyber incident reporting framework applicable across all categories of CNII operators.[3]

Many organisations remain reluctant to report cyber incidents because of concerns relating to reputational damage, financial consequences, regulatory sanctions and potential loss of customer confidence. This reluctance may result in significant cyber incidents remaining undisclosed, thereby limiting national awareness of emerging threats.

The absence of mandatory reporting requirements also affects the ability of cybersecurity authorities to develop accurate threat intelligence. Without reliable information regarding attack patterns, vulnerabilities and methods used by cyber criminals, government agencies and private operators may struggle to develop effective prevention strategies.[4]

A comprehensive cyber incident reporting framework should establish clear obligations regarding the circumstances requiring notification, reporting timelines, responsible authorities, information requirements, confidentiality protections and response procedures. Such a framework should balance accountability with cooperation by encouraging organisations to disclose incidents without unnecessary fear of punitive consequences. Effective reporting mechanisms should focus on improving national cybersecurity resilience rather than simply imposing penalties on organisations experiencing cyber-attacks.

8.4 Institutional Coordination Challenges

Nigeria's cybersecurity governance framework involves multiple institutions with overlapping responsibilities, including the Office of the National Security Adviser (ONSA), the Nigeria Data Protection Commission (NDPC), the Nigerian Communications Commission (NCC), the National Information Technology Development Agency (NITDA) and the Central Bank of Nigeria (CBN).[5]

[1] Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive).
[2] NIST, *Cybersecurity Framework Version 2.0* (2024).
[3] ENISA, *Incident Reporting for Digital Service Providers* (2021).
[4] Cybersecurity and Infrastructure Security Agency (CISA), *Cyber Incident Reporting Guidance*.
[5] OECD, *Digital Security Risk Management for Economic and Social Prosperity* (2015).

Each institution performs important functions within its respective area of responsibility. ONSA contributes to national cybersecurity coordination; NDPC regulates data protection; NCC oversees telecommunications security; NITDA supports information technology governance; and CBN establishes cybersecurity requirements within the financial sector. However, the absence of a single coordinating authority specifically responsible for CNII protection creates challenges relating to institutional overlap, information sharing and coordinated incident response. During major cyber incidents affecting multiple sectors, unclear responsibilities may delay decision-making and reduce the effectiveness of national response efforts.[1]

Effective CNII protection requires clearly defined institutional mandates, coordinated emergency response mechanisms, systematic information sharing and regular joint cybersecurity exercises involving government agencies and private operators. A fragmented governance structure may result in duplication of efforts, inconsistent regulatory approaches and delays in responding to significant cyber incidents. Therefore, Nigeria requires stronger institutional coordination mechanisms, possibly through the establishment of a dedicated CNII cybersecurity authority responsible for harmonising national efforts.

8.5 Limited Cybersecurity Capacity and Expertise

Cybersecurity protection requires specialised technical knowledge, yet Nigeria continues to face significant shortages of cybersecurity professionals, digital forensic experts, incident response specialists and cybersecurity researchers. These capacity limitations represent a major challenge because effective legal frameworks depend on individuals and institutions capable of implementing, monitoring and enforcing cybersecurity requirements. The complexity of modern cyber threats requires expertise in areas such as network security, artificial intelligence security, digital forensics, industrial control systems protection and cyber incident management. Without adequate human capacity, even well-designed cybersecurity legislation may fail to achieve its intended objectives.

Nigeria must therefore invest significantly in cybersecurity education, professional certification programmes, university research initiatives and government technical training. Higher education institutions should expand cybersecurity programmes that combine technical knowledge with legal and policy perspectives. Professional training programmes should also be developed to ensure that cybersecurity personnel remain updated on evolving threats and technologies. Furthermore, government agencies responsible for cybersecurity enforcement should receive continuous technical training to improve their ability to investigate cyber offences, analyse digital evidence and coordinate incident responses. Developing cybersecurity expertise is therefore not merely a technological requirement but a fundamental component of national security and infrastructure protection.

8.6 Challenges in Cross-Border Cybercrime Enforcement

Cyber-attacks against Critical National Information Infrastructure frequently involve international actors who operate beyond Nigeria's territorial jurisdiction. Attackers may conduct operations from foreign countries, utilise international servers, exploit multinational technology platforms or conceal their identities through sophisticated techniques. These characteristics create significant legal and practical challenges relating to jurisdiction, evidence collection, extradition and international cooperation.[2]

Traditional criminal justice mechanisms are often limited when dealing with cyber offences because digital evidence may be stored across multiple jurisdictions and investigations may require cooperation from foreign governments or technology companies. Nigeria must therefore strengthen international cooperation mechanisms through mutual legal assistance agreements, cybersecurity partnerships, intelligence-sharing arrangements and improved collaboration with international technology providers.[3]

Effective cross-border enforcement requires harmonisation of legal procedures, cooperation between law enforcement agencies and mechanisms for obtaining digital evidence across jurisdictions. Given the global nature of cyber threats, Nigeria's CNII protection strategy must recognise that domestic legislation alone cannot adequately address cyber risks. International collaboration remains essential for investigating offenders, preventing attacks and strengthening national cyber resilience.

[1] World Economic Forum, *Partnership Against Cybercrime Report* (2020).
[2] Global Cybersecurity Forum, *Cybersecurity Workforce Development Report* (2022).
[3] International Telecommunication Union, Cybersecurity Capacity Maturity Model for Nations (2021).

9. Recommendations to Strengthen the Legal Protection of Critical National Information Infrastructure in Nigeria

The preceding analysis demonstrates that Nigeria has developed important foundations for cybersecurity governance through the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (as amended), the Nigeria Data Protection Act 2023, the National Cybersecurity Policy and Strategy, and various sector-specific cybersecurity regulations. [1] These legal and institutional developments represent significant progress in recognising cybersecurity as a national security and development priority. However, the current framework remains inadequate to address the increasingly sophisticated, dynamic and interconnected nature of cyber threats targeting Critical National Information Infrastructure (CNII). Nigeria requires further legal and institutional reforms to strengthen protection of critical information infrastructure.

First, a dedicated CNII Protection Act should be enacted to establish clear classification procedures, operator responsibilities, cybersecurity standards and enforcement mechanisms.

Second, mandatory cybersecurity obligations should be imposed on CNII operators, requiring regular security assessments, incident response planning and compliance with international cybersecurity standards.

Third, Nigeria should establish a specialised CNII cybersecurity authority responsible for coordination, threat assessment, information sharing and national resilience planning.

Fourth, mandatory cyber incident reporting requirements should be introduced to improve national threat intelligence and coordinated response.

Fifth, stronger public-private partnerships should be developed because many critical infrastructures are privately operated. Government agencies, financial institutions, telecommunications companies and technology providers should collaborate through structured information-sharing mechanisms.

Sixth, Nigeria should invest in cybersecurity capacity development through education, professional training and research programmes.

Finally, cybersecurity reforms must respect constitutional rights, particularly privacy and freedom of expression. Security measures should operate within legal limits, with appropriate transparency and accountability mechanisms.

10. Conclusion

The protection of Critical National Information Infrastructure has become one of the most important legal and security challenges confronting Nigeria in the digital age. As government institutions, businesses and citizens increasingly depend on interconnected information systems, the security of these systems has become inseparable from national security, economic stability and public welfare.

This article has demonstrated that Nigeria has taken important steps towards developing a cybersecurity governance framework. The Cybercrimes (Prohibition, Prevention, etc.) Act 2015 provides the foundation for preventing cyber offences and recognising the importance of critical information infrastructure. The Nigeria Data Protection Act 2023 strengthens information security obligations and enhances protection of personal data. National cybersecurity strategies and sector-specific regulations further demonstrate Nigeria's commitment to addressing cyber threats. However, the existing framework remains inadequate for comprehensive CNII protection. The absence of dedicated CNII legislation represents a major regulatory weakness. Current laws focus primarily on cybercrime prevention and data protection but provide limited obligations concerning infrastructure resilience, cybersecurity standards, incident reporting and operational continuity.

Ultimately, cybersecurity protection is not solely a technological challenge but a legal, institutional and governance issue. Nigeria must therefore strengthen its regulatory framework through dedicated CNII legislation, improved coordination among cybersecurity institutions, mandatory security standards and stronger cooperation between government and private sector operators. The future security of Nigeria's digital economy depends on the ability of the state to protect the infrastructure upon which modern society increasingly relies. A comprehensive and rights-respecting CNII protection framework will not only reduce cyber risks but also promote trust, innovation and sustainable digital development.

[1] NIST, *Cybersecurity Framework Version 2.0* (2024).